PROPOSED LEGISLATION FOR CHINESE PERSONAL INFORMATION PROTECTION

A different approach from the European framework and other legislation?

Candidate number: 4

Supervisor: Professor Jon Bing

Deadline for submission: 01/12/2009

Number of words: 16,219 (max. 18.000)

29.11.2009

UNIVERSITY OF OSLO

Faculty of Law

Content

1 INTRODUCTION…….....1

1.1 Background.....1
1.2 Scope and motivation.....3
1.3 Resources.....4
1.4 Structure……..……....5

2 EU LEGISLATIONS ON DATA PROTECTION ……..……..6
2.1 Background…….....6
2.2 The Data Protection Directive.....10
2.2.1 Object and scope……..….....10
2.2.2 The main eight rules…….....11.
2.2.3 Special aspects..... 12

3 DATA PROTECTION IN CHINA TODAY……..……..14
3.1. Chinese legal tradition and historical background of “privacy”…….. 14
3.2. The foundation and features of drafting Chinese personal data protection law.....15
3.2.1 The Constitution guarantees the protection to the right to privacy……16
3.2.2 Other laws and administrative regulations and the decisions of the Standing Committee……16

4 DEFICIENCIES AND ALTERNATIVES FOR THE DRAFT OF CHINESE PERSONAL INFORMATION PROTECTION LAW.....19

4.1 Basic Situation and attitudes of the China law community……19
4.1.1 Current social status and problems of privacy protection……20
4.1.2 Present legal environment and limitations of personal information protection……...20
4.1.3 Tentative regional legislations on information protection……...22
4.2 Possible sources of a Chinese personal information protection law……..23
4.2.1 The US Model…….....23
4.2.2 The EU model……...24
4.2.3 The APEC Privacy Framework……26

4.3 The Proper Choice for China……..26

5 SCENARIO OF CHINA'S PRSONAL INFORMATION PROTECTION LEGISLATION ……..27

5.1 Basic structure and analysis of the draft of personal information protection Act of China.29
5.1.1 Scope, Definitions and Principles…….29
5.1.2 Executive mechanism……33
5.1.3 Remedies, Liabilities and Sanctions……..33
5.1.4 Exemptions and Restrictions……..34
5.2 Principal challenges to China's Personal Information Protection Law……...35
5.2.1 International recognition of China's personal information protection law……36
5.2.2 Scope of the data protection law……36
5.2.3 Handling of Sensitive personal data……..….36
5.2.4 International transfers of personal data……..37
5.2.5 Executive Mechanismsm……40

6 LEGAL PROPOSITIONS TO CHINA'S PERSONAL INFORMATION PROTECTION LAW…..42
6.1 On international recognition of China's personal information protection law.....42
6.2 On the scope of China's Personal Information Protection Law.....43
6.3 On the legislation of sensitive personal information.....44
6.4 On the issue of transborder personal information protection.....44
6.5 On the executive mechanism……...45

7 CONCLUSION……...48

BIBLIOGRAPHIES

1 Introduction

1.1 Background

The right to privacy and personal data protection are not new-launched concepts with the first definition dates back to more than 100 years ago.[1] The aim of data protection shares the same fundamental level of the concept of privacy protection. The new "information age" and "new information society" has posed us a brand new phase of data protection with many more ways of collecting, storing and distributing data personal data. The pivot of the challenge to the personal data protection processing is to shake the balance between individual perspective and social benefits.

Globally speaking, personal information has become such an important and valuable resource in the respect of business and public admimistration. To improve the utilization and protection of personal information, legislations in a global context have been established. The OECD Guidelines, as pioneers, is followed by EC data protection directive, Asia Pacific Economic Cooperation (APEC) Privacy Framework and also US's safe harbor agreement.

Data protection law grew up in Europe as a counter-weight to the threat to individuals' information privacy posed by the development of computers. Something similar is happening in China. As a major trading partner of EU and a growing robust economic entity on the world stage, China is embarrassed not to have a comprehensive national data protection law yet. However, as part of its rapid economic progress (which is reported with equal measures of admiration, envy and apprehension by the Western news media) it is rapidly expanding its infrastructure of information and communications technologies. Facing that China is sure to fail the assessment of "adequacy" requirement of personal information protection of EU, it urges China to formulate corresponding legislations so as not to be in a disadvantage stand in the EU market. The Chinese Government recognizes

[1] Warren, S.D and Brandeis, L.D,. The Right to Privacy, Havard Law Review, 1980, vol 4

the need for safeguards of the free data flow and is working on proposals for data protection legislation. As with many other jurisdictions, China will have to decide what form the legislation should take. Laws (or what the Anglo-Saxon world calls Acts) are passed by the National People's Congress (or Parliament). Regulations, which are subordinate to Laws, can be made by the State Council without the need to involve the National People's Congress. Both forms of legislation have effect nationwide, and it is not yet clear which route the legislators will follow. The easier and quicker course would be to make a regulation, but there are no doubt important constitutional considerations to be taken into account in making the decision. A further complication, at least when seen through European eyes, is that Provincial and Municipal authorities also have the right to legislate for their own areas of jurisdictions. For instance, Beijing city has shown some interest in legislating on data protection. In many judiciaries, it would be a recipe for chaos to have several tiers of legislation on a single subject, but China is such a big country with such a huge population that it is a fact of legislative life. For example, a number of provinces and municipalities already have laws permitting the public to gain access to government information (what is calledl freedom of information or public access to official documents in the Europe).

An early question that the Chinese policy makers and legislators will have to grapple with is what personal information should be covered by the proposed legislation. Even in Europe, which have had data protection legislation for many years, they are still trying to decide precisely what "personal data" means, and the Data Protection Directive's Article 29 Working Party has found it necessary recently to prepare a paper giving detailed guidance. [2]The China Daily article suggests that China may adopt a different approach from that followed in Europe.[3] It implies that, rather than using the general term "personal data", the proposed legislation may include a list of the various categories of information to which the legislation would apply. Personal mobile phone numbers, home addresses,

---

[2] Definition of personal data: In order to rectify a recent trend of divergence in the interpretation of the Data Protection Directive with respect to the definition of "personal data", the Working Party dedicated considerable effort and time to a detailed report on the concept of personal data.
http://ec.europa.eu/justice_home/fsj/privacy/news/docs/pr_20_04_07_en.pdf (accessed 25th, Nov.2009)

[3] Ouyang Wu, Director at the State Council Information Office, Strengthening Lawmaking Study on Personal Information Protection, and Promoting Personal Information Protection Lawmaking, Research on the Forefront of the Protection of Personal Information, Law Press China, 2006, p176

medical files, property documents and marital status are all mentioned as categories to be covered by the list. The danger of lists is that they may be not exhaustive. But this approach (if correct) is no doubt motivated by a wish to put the scope of the proposed legislation. As data protection professionals will recall from their own early experience, it is not easy to understand the breadth of information covered by data protection. This is also true for us in China coming new to the subject. There is one thing that is also important: in a country of 1.3 billion people, the prospect of managing a central registry of an unimaginable number of data controllers is, to say the least, daunting.

The Government works closely with selected partners in preparing its ideas and drafting legislation. Universities and other academic institutions are important sounding-boards. On the draft regulation on Access to Government Information, for example, selected academics were shown pre-publication versions of the draft law so that they could offer comments. It is probable that a similar approach will be followed on data protection. Indeed, the Chinese Academy of Social Sciences (CASS) seems already to have been closely involved.

1.2 Scope and motivation

As a country with a long history and unique cultural, social and, indeed, legislative traditions, China need not be bound by any pre-existing ideas or approaches. It has the opportunity to construct its own framework which best suits its particular requirements. The European model of personal information protection may affect China's proposed legislation - the approach enshrined in the Council of Europe Data Protection Convention, and the EC Data Protection Directive, albeit in a somewhat simplified form. Whether the Chinese authorities will find these recommendations persuasive remains to be seen. They may be drawn to the approach advocated by the Asia Pacific Economic Co-operation (APEC) group of countries which has prepared its own model for data protection regulation. There are also some in China who are attracted to the self-regulatory model exemplified in the arrangements for the "safe harbor" negotiated some years ago with the EU by the US authorities.

Up til now has not the draft of Personal Information Protection Act been adopted by the Chinese legislation, it still remains much to be amended and it raised much debate in China after its publication. It is such a contradiction that, on one hand, only if China establish a

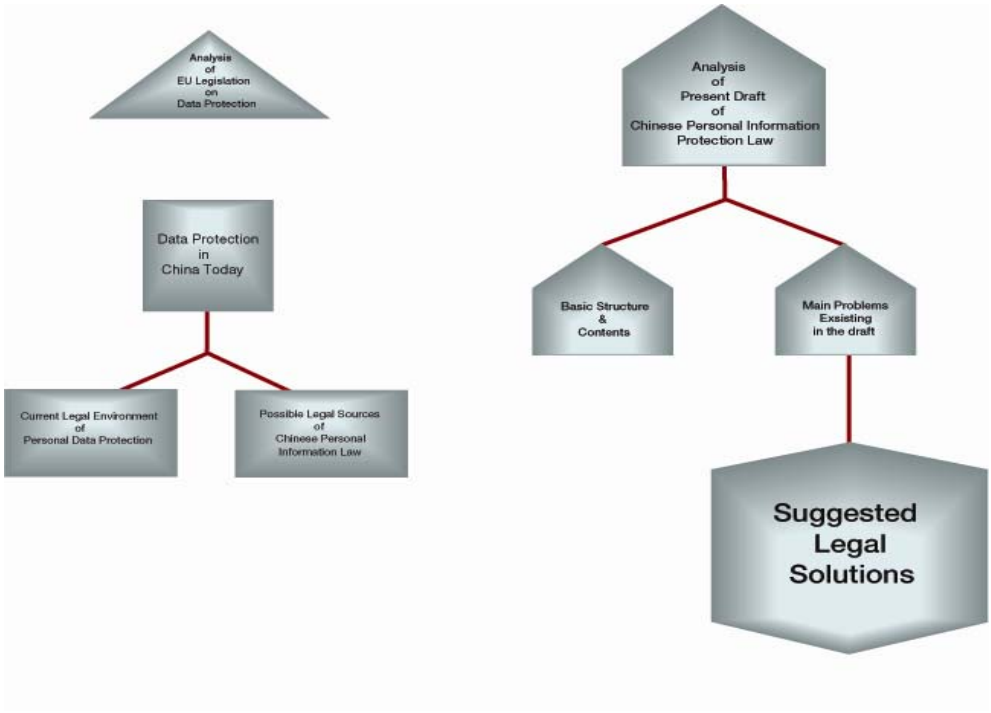
reliable and sound data protection regime will it ensure that the trade co-operation with most Western countries will develop. On the other hand, there seems to exist only a few systematic studies in the field, for instance, some fragmented personal papers and opinions even without an deserved number of researches and remarks on it.

There is no doubt that whether China, an indispensable economic and politic power of the world development, could provide ”adequate” personal information protection will have tremendous impact on the free flow of information and global market competition. As motivated by the great importance and sharp inconsistency of the data protection legislation in China, I would love to devote myself into the study of the legal environment of Chinese data protection which includes the difference between EU directives, opportunities and challenges to Chinese legislation and suggested ways of improvement on the data protection legislation.

1.3 Resources

The majority of the legal resources in my research lie in books, online articles, publications of professors, and official legal documents. On the part of EU legislation, I mainly refer to Directive 95/46/EC, the data protection directive. APEC privacy framework is also cited. Chinese data protection legislation draft, in particular, are the official report and the Chinese professors’ original work which will be translated by myself with the lack of official translation.

1.4 Structure



2 EU Legislation on Personal Data Protection

2.1 Background

In the late 1960s and early 1970s, the globe has seen the explosion of information power. The fear that computer age and information globalization might undermine human rights permeated the Europe. The fears are of different kinds. Trade would be fettered if information could not flow freely. Personal privacy and human rights might be weakened because of personal information and records invasion

The United States seems to be the first country to focus on privacy as a public issue,[4]triggered by the Nixon's Watergate case. Meanwhile in Europe, to respond to these fears, enforceable laws throughout Europe have been fomulated. The Swedish Data Act was the first national privacy act in the world, other countries framed their own national legislation successively by the end of 1980s. Many international initiatives have been adopted to protect privacy and personal data, which yield many agreements binding on many nations. Many international organizations such as The Council of Europe (CoE), the Organization for Economic Cooperation and Development (OECD) and the United Nations (UN) have adopted regulations and policies.

The Council of Europe was the first to draft a multilateral treaty dealing directly with protection of personal data.[5]The 1981 CoE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data aims to harmonize national laws and be a guide for domestic legislation. Moreover, the absence of rules for the flow of personal information from a party to non-party state was remedied by an Additional Protocol to the Convention with provisions data flow from party to non-party states.

---

[4] Bygrave,Lee A, International agreements to protect personal data, Global Privacy Protection, The first Generation, p4

[5] Supra footnote 4, p19

The OECD gave birth to the Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data in 1980. A set of eight core data privacy principles are proscribed to apply to manual and electronic processing of personal data in both private and public sectors. The Guidelines have no legal binding effects on OECD member states. However the OECD guidelines urge the member states to take appropriate legal measures for the "protection of privacy and individual liberties".[6] The OECD Guidelines and CoE conventions share the same standards in some respects that they do not require member states to establish data protection authorities. While the Guidelines supplement the Convention by urging member states to "encourage and support self-regulation, whether in the form of codes of conducts or otherwise".[7] The guidelines adopted a bulk of principles on privacy protection on global networks, having great influence on the enactment and content of data protection legislation in countries outside Europe.

The UN also adopted a set of Guidelines on privacy and data protection in 1990, which mainly includes two parts. Part A lays down minimum guarantees for inclusion in national laws, while part B encourages both governmental and non-governmental international organizations to process personal data in a more privacy-oriented way. It is noticeable that the UN Guidelines have some revolutionary principles which cannot be found in the CoE Convention and OECD Guidelines. The UN Guidelines emphasize the duty of data controller to do regular checks of the quality of personal data.[8] And the Guidelines insist that national protection authorities should be impartial, independent and technically competent.[9] The UN Guidelines aims to regulate data flows between a broader range of countries.

Nonetheless, among all these agreements, fundamental human rights instruments constitute the central basis for all data protection norms. Conspicuously, the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR) and European Convention on Human Rights and Fundamental Freedoms (ECHR) are considered to be of irreplaceable significance. Being the backbone of all jurisprudence

[6] OECD Guidelines para 6

[7] OECD Guidelines para 19b

[8] UN Guidelines para 2

[9] UN Guidelines para 8

developments, accordance to ICCPR Article 17 and ECHR Article 8 is considered to be the essential requirement of implementing basic data protection principles.

ICCPR Article 17 provides:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks upon his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.

The similar version in the Article 8 of ECHR provides:

1. Everyone has the right to respect for his private and family life, his home and correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health ormorals, or for the protection of the rights and freedom of others.

As individual countries were legislating for data protection, work was going forward on the development of international legal instruments. There was a perceived need for internationally agreed standards for data protection controls so as to ensure that discrepancies in the level of protection, or, indeed, the absence of data protection laws, did not hamper the free flow of personal data from one country to another. It was feared that countries with data protection legislation would prohibit personal data being transferred to countries with lower standards or no protection at all. This would be harmful to national economies and to the conduct of international transactions.

Significantly, deriving from the previous cited Article of EUHR, the European Union adopted its influential Privacy Directive, for eventual “ transposition” into the legal systems of all member countries. Today all these states are formally committed to the precepts of the 95/46/EC Directive.

95/46/EC Directive(hereinafter termed DPD) is firmly established as an internal market measure under Art. 95[10] which states that in order to achieve the objectives set out in art 14, that is to create an area without internal frontiers in which the free movement of goods, persons, services and capital[11] is ensured. Its utmost principle is to promote and facilitate world trade and international transactions in the manner of lawful free flow of personal information worldwide. It deemed to be the point of departure for national privacy and data protection initiatives within the EU, and outside Europe as well. The DPD placed a qualified restriction on flow of personal data protection from the EU to any non-EU member state who fails to provide "adequate" protection of personal data.

In addition to the DPD, the EU has formulated three other Directives regarding privacy issues directly. Directive 97/66/EC, dealing specifically with telecommunications was adopted in 1997. It has been replaced by Directive 20002/58/EC which is devoted to electronic communications. Later on, the EU adopted Directive 2006/24/EC on retention of telecommunication traffic data, which is mainly justified by terrorist attacks in London and Madrid. Known from website,[12] after three years' drafting, the Data Protection Framework Decision "*on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters*" (hereafter, the DPFD) was finally adopted on 27 November 2008.

The motivation for these laws was the developing use by the private and public sectors of increasingly powerful computers. The speed and ease with which computers could manipulate information, including information about people, was seen as posing a threat to individual privacy which existing laws were incapable of dealing with. The answer was to bring forward legislation specifically targeted on this problem.

---

[10] http://europa.eu.int/eur-lex/lex/en/treaties/dat/12002E/htm/C_2002325EN.003301.html

[11] See Recitals 3,5,7 of 94/46/EC Directive

[12] See online article "The data protection framework decision of 27 November 2008 regarding police and judicial cooperation in criminal matters – A modest achievement however not the improvement some have hoped for" 18 September 2009; available at http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6VB3-4X8524W-3&_user=10&_coverDate=09%2F30%2F2009&_rdoc=1&_fmt=full&_orig=search&_cdi=5915&_sort=d&_docanchor=&view=c&_searchStrId=1056379020&_rerunOrigin=google&_acct=C000050221&_version=1&_urlVersion=0&_userid=10&md5=e1e59775281146a5dc0bb344c11bf063 (accessed 10 Oct, 2009)

Elaborations will be made on the DPD, the first and only international privacy code to tackle directly the ambiguous issue.

2.2 The Data Protection Directive

After lengthy negotiations, Directive 95/46/EC was adopted in October 1995. Despite the impetus generated by the Convention, when the European Commission brought forward the first draft of the Directive in 1990, only about half of the then 12 EC Member States had data protection laws in place. The European Commission was concerned about the effect upon the internal market, which was then in prospect, of the lack of consistent data protection rules across all the member states. The Directive's principal purpose, therefore, was to create a "level playing field" throughout what is now the European Union so that one country could not use the lack of equivalent data protection laws in other member states as a reason for restricting or preventing the flow of personal data to those countries. The DPD also emphasizes the importance of protecting privacy in the respect of technological and economic developments.[13] Meanwhile, it reinforces and incorporates the law on human rights into the EU legal system.[14]

2.2.1. Object and scope

The DPD is unique in that it formulates regulations on the flow of personal data between EU members on the grounds of protection of privacy and other basic human rights (Article 1(2)). The Directive aims to set a "high" level of data protection, instead of a "lowest threshold" found in member states' existing internal laws. The Recital 10 of the DPD illustrates that it would like to strengthen and amplify the CoE Convention. (Recital 11).

The DPD lays down relatively wide and dynamic rules of privacy protection from an profound European angle. It applies to personal data processing in both private and public sectors. Processing of data on collective entities is not within the scope, however not prohibited by the member state's application. The DPD also provides for the law of an EU state to apply outside the EU in certain circumstances where a data controller is based

[13] See Recitals of 2, 3, 10 and 11 of DPD.

[14] See Article 1 of DPD. .

outside the EU but utilizes "equipment" in the state to process personal data for the purposes other than merely transmitting the data through tat state. [15]

Unlike the CoE, the DPD is not applied only in the automated processing of personal data. It applies also to the processing of personal data held in non-automated (e.g. paper) records which are part of a filing system (Article 3.1; Article 2(c)). The preamble to the Directive also makes it clear that the DPD applies to the processing of sound and image data (Recital 14). The DPD's scope cannot be wider than that of EC law itself, and certain activities are therefore exempted (Article 3.2, first indent). Subject to this, the only exemption is for processing "by a natural person in the course of a purely personal or household activity" (Article 3.2, second indent).

2.2.2 The Main eight principles

The key substantive rules are laid clearly in the DPD Article 6, which is known as the "Data Protection Principles". They play the pivotal role in the whole European legislation on data protection. In essence, they require the data to be

(a) processed fairly and lawfully;

(b) collected for specified, explicit and legitimate purposes and not further processed in a way which is incompatible with those purposes;

(c) adequate, relevant and not excessive;

(d) accurate and kept up to date;

(e) processed with the participation and control of the data subject

(f) restricted to the disclosure

(g) secured and not subject to unauthorized access, alteration, destruction or disclosure

[15] See Article 4(1)c, further referred to Global Privacy Protection P35

(h) controlled in a more stringent way concerning sensitive data .

The principles are elaborated upon in DPD Article 7 which sets conditions for the processing of personal data to be lawful; DPD Article 8 which sets additional conditions for the processing of special categories of personal data (generally known as "sensitive data"). Many of the principles in the DPD go considerably further than other international instruments. For instance, DPD Article 10 and 11 impose a requirement for basic information about the data-processing operation to be provided directly to data subjects. DPD Article 15(1) grants a person the right

"not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc."

Controversially it adds a new principle that fully automated assessment of a person's character should not form the sole basis of decisions that impinge upon the person's interests.[16]

2.2.3 Special aspects

DPD Recital 9 and Article 5 offer member states a "margin for manoeuvre". It remains to be problematic that member states'respective law is inconsistent with the Directive since they would rather preserve their own familiar rules.[17]

What's more, the DPD elaborates provisions on monitoring and decision-making regimes. Article 28 requires each member state to establish one or more "supervisory authorities" to monitor and help enforce the national law. The DPD also permits "prior checking" by data protection authorities of processing operations that are likely to present specific risks to the rights and freedoms of data subjects (DPD Article 20(1)).

[16] Supra footnote 4, P35

[17] Spiros Simitis, in 1995, made some telling observations of EU member states' attitudes during the lengthy gestation of the Directive, supra footnote 3, p33

The DPD anticipates high level of cooperation between the national data protection authorities, as is manifest in DPD Article 28(6). More importantly is that DPD Article 29 establishes a working party of representatives of data protection supervisory authorities from within the EU to monitor the application of the Directive and advise the European Commission. The working party has been very active and has a very influential role in developments in data protection within the EU. Moreover, Article 31 establishes a committee of representatives of member states' governments to assist the European Commission in its decision-making (which is primarily confined to decisions relating to the transfer of personal data to countries outside the EU).

The DPD emphasizes the strong control on the transfer of personal data to countries outside the EU (so-called third countries). DPD Article 25 ensures the basic rules on the requirement of an adequate level of protection, while "adequate" in itself is not specifically defined. And DPD Article 26 provides some derogation.

All 27 current member states now have data protection laws which are designed to give effect to the Directive. In 2003 (before the increase in EU membership) the European Commission published a report on the implementation of the Directive. The report suggested that one of the Directive's main aims – that of reducing obstacles to the free flow of personal data among the EU member states had been achieved – but that some problems remained. It identified three inter-related phenomena:

- inadequate resources for and emphasis on enforcement;
- patchy compliance by data controllers;
- low awareness of their rights by individuals.

3 DATA PROTECTION IN CHINA TODAY

3.1 Chinese legal tradition and historical background of “privacy”

It is noteworthy that the concept of privacy in its original Chinese sense has a large discrepancy from the western notion. Hence, it inevitably leads to the different legal culture and legislation background.

The notions of privacy are composed of distinct characteristics, qualities or elements in different jurisdictions.[18] In the traditional Chinese legal culture, it emphasizes more on the collective evaluationof individual’s rights, including the right of privacy [19] Right to personality of individuals in the history was never recognized and legally protected, not to mention the protection of personal privacy and information. The deep-rooted Chinese introverted mental state also hampers the step of chasing for personality and privacy right. Chinese people intend to view the word “privacy” as a synonym of “shameful secret”, which conotates a more disgraceful and negative notion. Chinese people were more inclined to make concession to avoid the realistic and legal troubles when their private rights were infringed. Being far different from the western idea, the concept of “collectivity” was more emphasized than “individuality”. Therefore, it caused the difficulty and conflict to make national legal recognition on the right to privacy and personal information.

The right of privacy is not viewed individually until 19th century. Now the Chinese jurisdiction and legislators treat the right of personality as a whole, namely, the right to reputation, image and privacy.[20] In the contemporary Chinese society, initial research on

[18] Bygrave,Lee A, Privacy Protection in a Global Context- A Comparative Overview, Scandinavian Studies in Law, 2004, vol.47, pp 319-348

[19] Cai Fang, On the Concept of Privacy in China and the West, Journal of Jiangse Polytechnic University Social Science Edition,2007,vol.2, available at:http://scholar.ilib.cn/A-jssyhgxyxb-skb200702006.html (accessed 10th Oct,2009)

[20] Yang Lixin, Discussion on Law of Personality Rights, Higher Education Press, 2005

right to privacy has an individualistic approach. As a private right in tort law, it means the right to be left alone or non-interference.[21]

3.2 The foundation and features of drafting Chinese personal data protection law

To support the development of the Information society and information industry in China, a strong consensus has been reached by Chinese government officials, the general public and legal experts that China needs to make regulations for the protection of personal data. Nowadays it is not simply a matter of the protection of personality rights. It has penetrated into different aspects of social and economic activities, especially those information-based industries like banking and insurance. With only a few fragmented and unsystematic regional regulations, many jurists and experts consider that the current legislation in China is far from sufficient and effective to keep up with the world pace of data protection and satisfy society's demands.[22] Such regulations are of relatively loose structure and with a limited scope of application. Furthermore, they lack a unified enforcing body and corresponding supervisory authority.

With over 20 years of sustained economic development, the financial and social conditions in China have improved greatly. According to the official statistics by 2009, China internet users soar to 298 million after surpassing the United States last year to become the largest.[23] Modern personal data collecting, processing, transmitting and use of the Internet not only promote economic and social development, which bring many benefits to people's daily work and lives, but can also bring about unprecedented threats to individuals. An online survey conducted last year showed nearly 89 percent of the 2,422 people polled claimed they had suffered because personal information had been leaked.[24] Anonymous messages, phone calls and spam were listed as the most reported means of harassment after personal information was made known to unauthorized agencies

[21] Zhang Xinbao, Legal Protection of Right to Privacy, Qunzhong Publishing Hose, 2004

[22] Feng Jianpeng, Brief discussion on rivacy protection in the information era, available at:http://chinalawedu.com/news/2004_7%5C19%5C1639588312.htm (accessed 10th Oct,2009)

[23] China's Internet Users Increased To 298 Million In 2008, available at http://www.chinatechnews.com/2009/01/14/8507-chinas-internet-users-increased-to-298-million-in-2008(accessed 15th Oct,2009)

[24] http://www.china.org.cn/government/NPC_CPPCC_2009/2009-03/04/content_17371338.htm

and individuals, according to the survey.[25] Lack of regulation to protect personal information had led to widespread harassment in China. People's spiritual concerns and protection of their personal interests is more urgent than ever. A privacy protection law or a legal explanation to clearly define the concept of personal information has become the top priority to the harmonization and sound development of the global economic activities.

As a matter of fact, some regulations on information and privacy have already existed in the Chinese legal framework.

3.2.1 The Constitution guarantees the protection to the right to privacy

The Constitution of PRC stipulates that the freedom and privacy of correspondence of citizens should be protected. Article 38 of Constitution of PRC states: "The personal dignity of citizens of the People's Republic of China is inviolable." Article 39 states that the residences of citizens of PRC are inviolable. Unlawful search of or intrusion into, a citizen's residence is prohibited. Constitution Article 40: "Freedom and privacy of correspondence of citizens of the People's Republic of China are protected by law. No organization or individual may, on any ground, infringe citizens' freedom and privacy of correspondence, except in cases where, to meet the needs of State security or of criminal investigation, public security or procuratorial agencies are permitted to censor correspondence in accordance with the procedures prescribed by law.

3.2.2 Other laws and administrative regulations and the decisions of the Standing Committee

General Principles of the Civil Law of the People's Republic of China Article 102 stipulates that citizens and legal persons shall enjoy the right of reputation. It protects the right of honor.[26]

The Supreme Court's explanation[27] about the compensation to the mental damage of the victim states by Article 1 (2) that If anyone violates the social public interest and the social

[25] Lawmaker, advisor urge for better protection of personal information**,** available at http://news.xinhuanet.com/english/2009-03/04/content_10940007.htm (assessed 15th Oct,2009)

[26] Article 102: Citizens and legal persons shall enjoy the right of honor. It shall prohibited to unlawfully divest citizens and legal persons of their honorary titles.

morals to violate the other people's privacy or other personal interests and the victim sues in the people's court by the reason of the infringement to request the compensation to his mental damage, the people's court must accept it according to the law.

Law of the People's Republic of China on Resident Identity Cards stipulates that Public security organs and people's police shall keep confidential citizen's personal information gained through making, issuing, examining or seizing resident identity cards. (Article 6(3)) The Law Article 19 states that Police must not disclose personal information obtained through examining identity cards.[28]

Postal Law guarantees the protection of freedom and privacy of correspondence and safety of the email.[29] Law of the PRC on the Protection of Minors provides the special group with protection against the breaching of privacy. The State Council also formulated the law that no person may disclose information identifying AIDS sufferers.[30]

E-commerce and general online activity has been developing rapidly in China. Unfortunately, given the relatively lengthy time it takes to enact national laws in China, the legislation has not kept up to date with these developments. Although China lacks major privacy and data protection laws as discussed above, some regulations are in place in relation to network information. The Regulation on Management of the Administration of

---

[27] It is controversial about its effect in terms of jurisprudence. However, in reality, it is defined that the explaination made by Chinese Supreme Court is of legal effect of enforcement once is pulicated. http://www.court.gov.cn/html/article/200810/27/772.shtml (available at 20th, Nov. 2009)

[28] Article 19 of Law of the People's Republic of China on Resident Identity Cards: Any police officer who commits one of the following acts shall, according to the seriousness of the circumstances, be given administrative sanctions in accordance with law; and if a crime is constituted, he shall be investigated for criminal responsibility in accordance with law: (5) divulging a citizen's personal information gained through making, issuing, examining or seizing his resident identity card and thus infringing the citizen's lawful rights and interests.

[29] Article 4 of Postal Law: Freedom and privacy of correspondence shall be protected by law. No organization or individual shall infringe the freedom and privacy of correspondence of other persons for any reason, except when the inspection of correspondence in accordance with legal procedures by the public security organ, the State security organ or the procuratorial organ is necessary for the State's safety or the investigation of a criminal offence.

[30] Article 39 of Regulation for the protection to AIDS: When disease control and prevention organizations and the enter-exit inspection and quarantine organizations carry out HIV / AIDS epidemiology investigation, the bodies and the individuals inspected should offer the relevant information according to the facts. No organization or individual should publish the name, address, occupation, and profile, materials of the medical history of someone suffering from AIDS or information that allows their personal identity to be known.

Internet Electronic Messaging Services issued by Ministry of Information Industry on 8 October 2000 is worth looking at. Article 12 states that Electronic Messaging Service providers shall maintain the confidentiality of personal information concerning online subscribers and may not disclose the same to third parties without the subscribers' consent.

The growing use of internet and e-mail encouraged the legislation on the personal information protection of the network users.[31] Likewise, to respond to the urgent demands of the electronic market, the People's Bank of China made the regulation that banks must keep secret individuals' credit information.[32]

As is obviously observed from the existed provisions in Chinese legal framework, the laws and the administrative regulations demonstrated above do cover data protection to a limited degree. Without a comprehensive data protection law, the existing provisions only give static, rather than expected dynamic, protection to personal data in different aspects and in different areas.

At present, China is drafting a new Civil Code; the privacy issues are introduced as follows in the latest draft: "Natural persons enjoy privacy; privacy is constituted by personal data, personal activities and personal space; collection, saving and publication of personal data, shall be consented to by the data-subject in all cases". It is hoped that guidelines will be developed around the new Code, similar to those that are seen operating in Hong Kong under its Data Protection Ordinance.

[31] Article 4 of National People's Congress Standing Committee's decision on safeguarding Internet security: Any of the following acts which constitute a crime will be prosecuted for criminal liability in accordance with provisions of the Criminal Law: illegally intercepting, tampering with and deleting e-mail or other data materials of others constitute an infringement of freedom and privacy of correspondence.

[32] Article 5 of Interim Measures to administrate the basic database of the personal credit information: The People's Bank of China and commercial banks should keep secret the personal credit information which they get through their work. And Article 6 of the Regulation of the PRC on Commercial Banks: Commercial banks shall safeguard the legal rights of depositors against infringement from any units or individuals.

4 Deficiency and Alternatives for the Draft of Chinese Personal Information Protection law

4.1 Basic Situation and attitudes of the China law community

4.1.1. Current social status and problems of privacy protection

Under the fast growth of the macro environment of the world network technology, the transfer, processing and utilization of information has become paramount factors in success of world market. Internet and communication net are important carriers of saving, delivering and publicizing personal information. “Informatization is the mega-trend of world development and a key factor in promoting social and economic development and reform.”[33] As such important social resources, they are so easy to be leaked illegally and used in inappropriate and unreasonable way. In this e-commerce world market, the internet and online information make the economic activities all the more globalized. Electronic business, such as B2B, B2C, electronic contracts and e-payment is growing robustly in both international and domestic trade. To promote a healthy economic growth, General office of the CPC Central Committee and General Office of the State Council has published The State Informatization Development Strategy.[34]In this project, the regulations on e-commerce, e-government, protection of personal information and information security are attached great importance to. It is worth noticing that it is the first time that the demand of legislation on personal information protection is listed in a national development guideline of Chinese government. Chinese government has paid unprecedented attention to personal information protection in its state strategy. Working Plan of Working Term on National Information in 2004 has suggested that the formulation of Electronic Signature

[33] Wen Jiabao, Prime Minister of China, said at the fifth meeting of the National Leading Group on Informatization

[34] It defines ”informatization” as a history course of developing and making use of information resources on the basis of information technology, promoting information communications and share of knowledge, in order to enhance the quality of economic growth and propel development of economic society. See the State Information Development Strategy(2006-2020), May 19, 2006 available at: http://www.cnii.com.cn/20050801/ca350966.htm (accessed 16 Oct, 2009)

Law, a draft of Personal Data Protection Law and Regulation on Internet Information Security. Though the conflict between privacy protection and information flow may be not so sharp in China currently, it is outstanding enough. They two not only contradict themselves but also facilitate each other to obtain the "win-win" situation if treated properly.

On the part of China, we have already been in the face of numerous vexing problems in privacy and data transfer issues. In 2000, a famous net company named "Netants" was reported to disclose its customers' information to some overseas companies, which caused sensational effect in the society.[35] However, it was ended for the reason that no substantial proof was found. But what will Chinese legislation react if the case was brought to the court? Likewise, there are a lot of cases on violation of privacy rights. To name one recent case, it is reported that the inproper internet search for human flesh search engine did lead to a lot of disputes. A girl sued the website company for their violation of her reputation.[36] Human flesh search engine is a new-rising online searching method, which makes searching more vivid and effective, especially in searching for a person. Meanwhile, it makes personal information more easily disclosed and misused. This kind of case is by no means rare today. It is happening every day. However, the lack of corresponding jurisdiction and applicable law complicates the matter and poses threat to the citizens and trouble to the legal workers.

There exist some common problems in our daily life such as unsolicited marketing material spam and advertisements, misuse of information, illegal market in transferring personal information. What's more, the loss of database may cause identity fraud. Data subject cannot really control their information.

4.1.2 Present legal environment and limitations of personal information protection

Being the fact that right to privacy has not been recognized as an individual's natural legal right in either Constitution or any statues, it resulted in the regulatory vacuum in privacy

[35] "Should Share Software be responsible for its users", Popsoft Magazine, 2000, vol. 16, p10-15

[36] Case study: Discussion on personal privacy from the aspect of human flesh search engine. Available at http://www.chinaret.com/user/topic_view.aspx?id=b7a9dcd6-3827-4f83-8a4a-431d2b1514fa (accessed 15,Oct,2009)

and data protection. While, some judicial interpretations by issued by the Supreme court of China has been applied in dealing with some cases. Take "opinions of the Supreme People's Court on Several Issues concerning the Implementation of the General Principles of the Civil Law of the PRC(for trial implementation) as an example, it made detailed provisions on the case decisions involved infringement of the right to privacy. (Article 140, 141) [37]

Admitted that there are several regulations and legal interpretations on privacy protection, none of the fundamental Chinese laws guarantees the right to privacy as an independent right of personality. Even not an article gives clear definition on privacy. Many basic questions are left unsolved: What is personal information? What kind of privacy should be regarded as protected? What sort of personal information can be legally used? Under which situation can the information reasonably and legally be used? How to deal with the illegal use of personal information? Currently a number of privacy cases are approached by applying the article of infringement of right to reputation under the general civil law. Nevertheless, those two rights are not on the same ground. The violation of reputation right in Chinese legislation is an ad hoc regulation, which renders the burden of proof on the plaintiff. Therefore, it is not reasonable to substitute the right of reputation for the right of privacy.

Besides that, there is no specific corresponding managing mechanism in regard of personal information access, collection, use and marketing. [38] In accordance with the current Chinese law, where personal information is violated, the liability is limited to administrative and criminal responsibilities. The lack of a corresponding compensatory system makes the matter difficult to control. It still lacks a clear definition on the compensation of the right to privacy in the Interpretation on Problem regarding the

[37] Article 140: Those who disclose other's privacy defame other's personality by fabricating the facts publicly, or damage other's reputation by indignity and humiliation in oral or written forms shall be deemed as infringement of citizen's right to reputation.

Article 141(1): Those who causes damage of other's right to reputation by invasion of right to privacy, shall bear civil liability as infringement of right to reputation.

[38] Li Changxi, Internet Law-making of Personal Information Protection in China, Research on the Forefront of the Protection of Personal Information, Law Press China, 2006

Ascertainment of Compensation Liability for Emotional Damage in Civil Torts enacted by the Supreme Court of PRC in 2001.

The legal community in China is generally responsive to establishing a personal data protection law or regulation, and believes that it is necessary for China to establish such a regime for strengthening the protection of the fundamental rights of individual citizens, promoting the development of industry to meet international requirements. Despite this general support, the actual number of legal experts who have conducted in-depth research in this field is very small. Personal data protection is a new field, which requires researcher to have plenty of related knowledge. Legal experts with extensive knowledge of the traditional area of private or public law may still be in need of additional training in order to be able to develop proper amendments to the Chinese legal system.

The Chinese legal authority did respond to the urgent situation. Around the year of 2003, a group of academics from the Chinese Academy of Social Sciences were gathered to research and prepare a draft data protection law. A draft law was finished in 2005 and later published. However prospects later became less clear after a ministerial reorganization of many of the agencies and bodies involved. At the time of writing, prospects of when such a law may be enacted remain unclear.

4.1.3 Tentative regional legislation on personal information protection

In practice, a number of local authorities have already done a faily useful explorations in some big leading cities of China. Beijing, Shanghai, Jiangsu, Zhejiang, Shenzhen and some other places have issued administration methods on publicity, collection and use of credit information. Among them, Shanghai and Shenzhen specially regulated the use of personal credit information and issued Pilot Scheme of Administration of Personal Credit Rating, and Administration Approaches of Personal Credit Rating and Credit Appraisal.[39]These regulations have played an effective role in promoting social credit system and fiduciary achives of the citizens and accumulated experience in advancing national legislation.

[39] Supra footnote 38, Wang Shengli, Social Credit System and the Protection and Publicity of Personal Information, P204

4.2 Possible sources of a Chinese personal information protection policy

4.2.1. The US Model

The legislation of the US data protection bears the characteristics of diversity. It has a number of legal resources, which also reflects the government system of separation of the powers. The application of privacy protection varies from one to another sector. It depends on the activities whether it is governmental or private. The US privacy law demonstrates the balance between the benefits and the burdens of the protection.

The DPD would prohibit the transfer of personal data to non-European Union nations that do not meet the European "adequacy" standard for privacy protection. While the United States and the European Union (EU) share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy from that taken by the European Union. As a result of these different privacy approaches, the DPD could have significantly hampered the ability of U.S. companies to engage in many trans-Atlantic transactions. In order to bridge these different privacy approaches and provide a streamlined means for U.S. organizations to comply with the Directive, the U.S. Department of Commerce in consultation with the European Commission developed a "safe harbor" ramework. The safe harbor—approved by the EU in 2000—is an important way for U.S. companies to avoid experiencing interruptions in their business dealings with the EU or facing prosecution by European authorities under European privacy laws. The key notion of the Safe Harbor approach is to provide joining organizations wiht a presumption of adequacy in order to ensure the continuation of data transfers from the EU.[40] Certifying to the safe harbor will assure that EU organizations know that your company provide "adequate"privacy protection, as defined by the Directive.[41] This agreement only applies to personal data traffic coming from the EU to the US. There is a system for domestic personal data protection in the US. It does not primarily rely on government intervention, but starts from a perspective of constitutional protection for private property. Publishing personal data is often also seen as falling under the constitutional principles of protecting freedom of expression. This system assumes that an

[40] Roland Vogl, The EU-US Privacy Controversy: a Question of Law or Governance?, May, 2000, p8 http://www.law.stanford.edu/publications/dissertations_theses/diss/VoglRoland-tft2000.pdf (accessed 10th, Nov.2009)

[41] http://www.export.gov/safeharbor/eg_main_018236.asp (accessed 10th, Oct, 2009)

individual must reveal to some degree personal data in order to foster trade and competition. And the American government enhances the protection of the right to privacy by resorting to the technological progress and the invention of the related protective programs.

The US adopted this model for two reasons.

(1) The US-American legal culture focuses on individualism and the function of the constitution and the basic position of the right to privacy in protecting people's rights. The government should not intervene if existing regulations can settle matters.[42]

(2) There exists the tense imbalance between individualism and public interests in the society. The US model chases the maxim of both the individual and public interests. It tends to use the minimum cost to achieve the best balance between both the personal protection and public interests.

4.2.2 The EU Model

The European Commission's Directive on Data Protection went into effect in October, 1998, which benefits a lot to the European citizens. The EU model is designed to protect personal data through government-led approaches. According to the DPD Article 25 and Article 26, Member States will be allowed to transfer the personal data to third countries only if the third country in question ensures an adequate level of protection. Regarding enterprises, the adequacy level standard increases the confidence of the consumers and the growth of online business as well. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances of the transfer. If a third country does not ensure an adequate level of protection, the member states of the EU shall take the measures necessary to prevent any transfer of data of the same type to the third country in question. Under that circumstance, China's level of protection could be assessed when such a business is involved.

However, the DPD needs to be desired in many aspects. To begin with the principles on which to decide whether the DPD can be applied in specified processing are too complicated and indefinite. Moreover, the coordination with different member states is not

[42]Supra footnote 38, Fred H.Cate, Privacy Protection of the US, P101

effective, thus influencing the principles of data processing of different countries. Honestly speaking, the directive hasn't played the expected role but adds burden to the data processing department instead.

The main differences between the US model and the EU model are as follows:

(1) Supervisory measures: The EU model may also be called the "unitary" model, in which a special organization, which has an independent investigative power, is established. The US model may also be called a "decentralization" model, in which the supervising organizations are scattered in various relevant bodies. For example, medical information and financial information are supervised by relevant bodies.

(2) Supervisory model and manner of personal data protection by the commercial organization and the public organization: In order to balance the protection and the flow of data, the emphasis of the US model and the EU model are placed particularly in different fields. More emphasis is placed on data protection in the EU, but in America the emphasis is on self-discipline in the commercial organization and on regulating public bodies.

(3) Processing of sensitive data: US and the EU model have different ways in the determination of the scope of sensitive data, though they both concentrate on it.

(4) Resources of legislation: The United States uses a sectorial approach that relies on a mix of legislation, regulation, and self-regulation. The European Union, however, relies on comprehensive legislation that, for example, requires creation of government data protection agencies, registration of data bases with those agencies, and in some instances prior approval before personal data processing may begin. Regarding the provisions of personal data protection in the US, their scope is not comprehensive, and heavily relies on self-regulatory efforts by the data processors. The EU system, in contrast, relies primarily on a legal framework and statutory controls, with self-regulation being possible as a complementary solution.

4.2.3. The APEC Privacy Framework

Asia-Pacific Economic Cooperation (APEC) is the premier forum for facilitating economic growth, co-operation, trade and investment in the Asia-Pacific region. The APEC Privacy Framework was developed from 2003, adopted in 2004 and finalized in 2005.[43] It could have become the most influential international privacy instrument since the EU Privacy Directive 1995, aiming at improving the standard of information privacy protection throughout APEC member states and facilitating the transborder flow of personal information between these countries. The APEC Privacy Framework has been put forward as a foundation on which to build a global privacy framework. It serves to be a practical policy approach to enable accountability in the flow of data while preventing impediments to trade. It provides technical assistance to those APEC economies that have not addressed privacy from a regulatory or policy perspective.

The Framework comprises a set of nine "APEC principles" in Part III, "Implementation" in Part IV, finalizing section B in 2005 on the issue of "cross-border elements". While Section B says nothing directly about personal data exports either in terms of limitation rules or requirements to allow them.[44] Basing itself on the OECD Guidelines, the APEC nine privacy principles deal with topics normally found in international or national sets of privacy principles. However it is often criticized that its principles are much weaker than the OECD Guidelines, the EU Directives or most existing data protection laws in Asia Pacific and no substantial enforcement requirements. The final version of the framework does not explicitly stand as a strong position.

4.3 The Proper Choice for China

It is suggested by most of the jurist experts that China should adopt the model combining the both the EU and the US model. Chinese legislation model on data protection should absorb both of their essences while in accordance to China's basic social and political

---

[43] Graham Greenleaf, Five years of the APEC Privacy Framework: Failure or promise?, (2009) *Computer Law & Security Report* 25 CLSR 28-43 http://www.sciencedirect.com/science?_ob=MImg&_imagekey=B6VB3-4VHYRH6-5-1&_cdi=5915&_user=674998&_orig=search&_coverDate=12%2F31%2F2009&_sk=999749998&view=c&wchp=dGLzVzz-zSkWA&md5=f8e761ab03ee1942a8f02c32790bc0ad&ie=/sdarticle.pdf (accessed 15th, Nov. 2009)

[44] Supra footnote 43

situation. Judging from China's current legal and social environment, it appears more reasonable and feasible to base a personal data protection regime on EU approaches to data protection – with necessary modifications accommodating for China's specifics in law and administration, and also to allow for Europe's experiences with implementation of its provisions over the past decades. In particular, Chinese data legislation model would go more towards the EU model in view of the following manners:

The starting point for reflections about which of these practices can be recommended to the Chinese government to adapt and adopt is the assessment that the EU personal data protection regime has proven to be a very robust one: it was able to accommodate the omnipresence of electronic means of communication as well as globalization on any level. It could be teamed with most of the European governments' efforts to improve government service quality, efficiency, accountability and credibility by introducing transparency programmes and freedom of information laws. That it is capable of being applied in countries with a wide variety of social, cultural, and legal traditions is demonstrated by its broadly successful adoption in the 27 member states of the EU.

Since there is no existing legal system to protect personal data, a fully-fledged EU framework will be set as a comprehensive good model. Relatively speaking, this solution has provided the highest level of protection to personal data and received the vast popularity. Seen from economic angle, as the biggest trading partner of the EU, China must pay attention to meet the international norms, especially EU "adequacy" level for the protection of personal data so as not to be restrained by the flaws in the handling of international data flows. The equal guarantee of data protection will benefit the growth of bi-lateral or multi-lateral trade and economic activities.

In addition, China is also a country whose legislation is based on laws and statues instead of cases and self-regulations. China is under the same regime as European civil law, rather than case law. The legislation, enactment and compliance of the law in China all need discreet and precise statutes and code. Consequently, the EU model constitutes a fairly reasonable model of legal reference regardless of some deficiencies.

Moreover, there is not yet a strong tradition in China of entrusting industry and professional organizations with self-regulatory tasks and the necessary authority to assume responsibility from the government. In the specific case of data processing industries, it appears that industry associations do not yet have the necessary capacity to establish and implement this kind of self or co-regulatory system.

5 Scenario of the draft of China's personal information protection law

There is no such thing as a perfect solution to the matter of privacy protection of such complexity. Even if the EU directive is significant, it is far from being an exact model of legislation to follow but sets a common standard for the protection of personal data.

As urgently requested by the citizens and international trade growth, Chinese government is marching on the way to a fully-legislated democratic legal society. Realizing the indispensability of the protection of personal information and the significance it will bring to the social benefits and economic interest, China started the research and legislation step by step. In the beginning of 2003, State Council Information Office entrusted the research team on personal information protection law in Legal Research Institute of Chinese Academy of Social Science to do research on “Personal data protection law of China” and to draft the proposed act. In 2005, the draft was initially completed and submitted to the State Council Information Office. Then it is publicized as personal information protection Act of China (experts on) with its Legislative Study Report. Now State Council Information Office has the capacity to formulate a formal draft instead of proposals from experts. Whether and when the final draft will come to the stage still remains indefinite. However, it was confirmed that the formal draft will be designed on the basis of the draft submitted by the experts in 2005. Though there is no further news on the draft of the 2005, it does stand out as a blueprint of the would-be model of formal Chinese Personal Information Protection Law.

5.1 Basic structure and analysis of the draft of personal information protection Act of China

5.1.1 Scope, Definitions and Principles

The scope of the application of the law of personal information protection looms to be one of the most important matters of all countries in the process of legislation. It involves the decision and choice of two main aspects: first, choice between public and private sectors;

second, choice between computer processed information and manually processed information.[45] Regardless of the wide difference in the first choice, the Chinese legislation views that it must apply the law to protect both the private and the public sector. From the perspective of personal information protection, it makes no difference to protect public sector or private sector, as long as they both manage a large amount of personal information and have the possibility of imformation and privacy misuse or offense of individual rights.

In the Chinese Personal Information Protection Act (Experts On) (hereafter refers to the Act), the scope is approached on two sides. On the one hand, there are provisions equally applicable to both private and public sectors. On the other hand, different obligations are regulated for governmental agencies and other personal information processors.

In respect to the choice between computer processed information and manually processed information, the Chinese draft adopts the common practice by stipulating that the law is applicable to information either processed by computer or manually. In China, due to its long history of data and archive management system, it is impossible to have all the personal information computerized or automated. The clarified equal application to the manually processed information not only reduce the uncertainty in its scope and prevent legal circumvention, but also protect substantial individual rights. Moreover, the draft adopts a universal practice in limiting the manual processing of personal information to "certain arrangements or searching standards"[46], rather than to all manually processed information.

Meanwhile, the definition of "governmental agencies" in the draft follows the subject definition in the Administrative Reconsideration Law and the Administrative Litigation Law. That means, besides the governmental administration authority, other administrative subjects executing administrative functions or providing public services shall also be

[45] In few numbers of countries, it might be the third kind of choice that is the choice between personal information and legal person's information, such as Argentina.

[46] Article 9 of Personal Information Protection Act (Experts on)

included into the category.[47] The Experts on tends to define the "personal information processors" in broad way. Any individual, legal person or organization processing personal information in accordance with provisions in the personal information protection law shall fall into this category and shall be subject to legal restrictions on an equal footing.[48]

The Act adopts the notion of personal information instead of privacy or personal data for the reason that the latter two have ambiguous meaning in the background of Chinese tradition and culture. The draft chooses neither the concept "personal data" from EU model nor the "privacy" from the US model. The definition of "personal information" of Chinese draft symbolizes an independent voice which will be favourable for China in the international trade and international communications.

The definition in the draft is expressed that the information, which can alone or in reference to or in comparison with other information, identify a specific person, such as a person's name, residential address, birth date, identification card number, medical record, personnel record, photograph, and etc.

The definition of "processing" is not the same notion as it is in the EU directive. It is defined that the collection, storage, usage, exchange, disclosure, modification, deletion and destruction and other treatments on personal information conducted by governmental authorities or other processors by automatic or manual means in accordance with certain standards of layout or searching methods.
The core principles which shall be abided by both government authorities and individuals are provided in the General Principles of the Draft. While some different respective principles and norms are formulated in the Chapter 2 and 3 due to different legal status.

The seven basic principles are:
a. Principle of lawfulness
b. Principle of Protection of Rights
c. Principle of Balance of interests

---

[47] Zhou Hanhua, Personal Information Protection Act of China(Experts on) and the Legislative Study Report, Law Press China, 2006, p54

[48] Supra footnote 47, p55

The protection of personal information shall neither impede other's rights and freedom, nor harm the national or public society's interests.

d. Principle of Information Quality

e. Principle of Information Security

f. Principle of Professional Duties

The staff of government authorities or other information processors should be responsible for the confidentiality of the personal information they process during the period of their tenure. They shall not inform others or otherwise disclose or use it on their own volition without the authorization of others.

g. Principle of Remedy

The subject is entitled to apply for administrative remedy or commence litigation where they believe the processing by the government authorities or other information processors is unlawful or infringe his legal rights and interests.

Government authorities or other information processors shall bear the liabilities for damage from their illegal processing.

Individuals, legal persons or other organizations are entitled to apply for administrative reconsideration or administrative litigation where their legal rights are infringed by a specific administrative act of government information resource department.

The last two principles carry the special characteristics of China's national situation. The principles attach great importance to protect personal information from the invasion of public authority.

However, it is disappointing that the Draft lacks principles regarding the processing of sensitive personal information. Moreover, in comparison with widely-accepted principles of international instrument, the draft has such principle as: a) secondary use should occur only with the consent of the person or by authority of the law; b) the amount of personal information collected should be limited to what is necessary to achieve the purpose for which data is gathered and processed.

5.1.2 Executive mechanism

It is a decisive factor to the successful and effective enactment of information protection law. The DPD Article 28 specifies the function and power of national supervisory authority. According to this provision, most EU member states have set up supervisory

authorities. For example, Denmark has set up an independent data protection agency. But APEC Guidelines hasn't involved any special provision on enforcement agencies. Another example would be Japan. When formulating its personal informaiton protection law, it pointed out that it may greatly restrict the freedom of non-public sector.Thus they suggest an effective system of after-fact assistance.

As a matter of fact, up till now China has no specialized government department or independent agency which is in charge of government information resources. It is prescribed in the draft that the government information resources department is the executive body. Nevertheless, the vague term government information resources department has no detailed definition of what form it will take, what functions it will carry. The independence, specialty and authority of the executive body rely on clarified definition, responsibility and function.

5.1.3 Remedies, Liabilities and Sanctions

On the basis of the principle of remedy, the draft regulates the corresponding legal remedies, penalty, civil relief and sanctions involving the violation of personal information. It is often the case in China that laws and regulations are not completely complied and strictly implemented. The practice that using forfeiture or penalty instead of formulated sanctions is quite common.[49] Therefore it is difficult to ensure the legal effect of the enactment of civil remedy and administrative measures. Especially, under the current situation, infringement of personal information is a new issue for the public and government agencies. In order to ensure the enforcement of the draft, criminal sanctions are emphasized in Chapter 5.[50]

However, there exists no direct regulation stipulating the criminal responsibilities arising from the infringement on personal information rights. Consequently, the enactment of criminal sanctions needs specified stiputlation in the criminal law. For instance, the investigation of criminal responsibilities of the staff of government information resources

[49] Supra footnote 47, p90

[50] Article 65-68 of the Chinese Personal Information Protection Act (Experts on), the staff of the government information resources department will be given administrative punishment where one of the following cases occurs. Criminal responsibilities will be constituted whereas the case constitutes a crime.

department can apply the regulations of professional crimes of public officials, such as corruption and dereliction of duty. The concrete enactment of criminal responsibilities shall be further elaborated by judicial interpretations of the Chinese Supreme Court.

5.1.4 Exemptions and Restrictions

From a jurisprudential perspective, exceptions and restrictions are necessary prolongation of the law's scope of application. Nearly all the codes of various nations try hard to balance personal information protection against other personal rights and freedom and public interests. Some legislation defines it in a general way, namely DPD Article 3. Some formulate it in an enumerative manner, namely Icelandic Personal Data Protection Law Chapter 5 and Swedish Personal Data Law Chapter 7.[51] Yet no matter if it is general or concrete, the scope of exception covers national security, news press, scientific research and pure personal information processing. The exceptions and restriction can be mainly divided into two levels: absolute exception and restrictive adoption. The former is deemed as prior system with clear regulation scope which is frequently applied with national security. While the latter is categorized as *ex post facto* sanctions for breach of data protection laws, which leaves executive body much room for balancing interests according to specific cases mainly of medical treatment, new press or literary products.

With an aim to balancing the personal information protection against public interests and keeping necessary flexibility and intensity of law, the Chinese experts adopt a combination of unified absolute exclusion beforehand and plural restriction after-fact.[52]
Article 10 of the General Rules of the draft regulates three main categories of exemptions on the application:
a) National security agencies using personal information processing for security protection purposes, the scope of which shall be defined by the State Council;
b) Personal information processing that related to pure individual or family activities
c) Personal information processing activities by legal person or organizations with limited quantity and little possibility to infringe personal rights, the scope of which shall be

[51] Supra footnote 47, p57

[52] Supra footnote 38, p233

determined by specific regulations made by government agencies that take charge of information resources.

It has been argued about the third type that neither clear standards nor procedural restrictions exist. In addition, the information and resource department of the State Council will be assigned too much power that may lead to abuse. However the experts believe that they have justified reason to maintain this exemption provision. The assumption is based on the reason that: first, the government information resource department does possess great power, but when exercising the power, they have to follw regulations which were made through formal proceedings and by legitimate forms. Second, under the current Chinese legal structure, there are manifold monitoring systems against agencies' policy-making activities, including legislative, administrative and judicial supervision. On condition that all supervisory mechanism fully performed their role in the balance, power abuse can be prevented effectively.

Besides the general rule, the draft formulated detailed provisions in Chapter 2. Article 12 stipulates the cases of collection of personal information by government agencies which are restrictions. The third item involves that the administrative penalty and administrative enforcement are excluded from the scope of the draft, which gives the administrative bodies much self-determination on the judgment of the cases. This provision will easily result in power abuse and infringement of personal information rights. Article 15 further provides the conditions that fall out of the scope of the act. Especially item 8 states a controversial exemption on the processing of personal information that are only used in the interior government agencies with justified reasons. There is no further interpretation and legal provisions to specify what is lawful and justified. The rest of the provisions of the exemptions are similar to the EU Directive.

5.2 Principal challenges to China's Personal Information Protection Law

5.2.1 International recognition of China's personal information protection law

There are a few leading questions that should be solved for China to set up a comprehensive personal information protection law. What provisions should China's data protection law contain to ensure an "adequate" level of data protection? What is considered to be "adequacy" is not specified in the DPD and by its Article 29 working

party. However, the provisions are made by the European Commission in consultation with other EU member states. As a third country to EU, Chinese legislation might be formulated based on the view of an EU data controller in order to satisfy minimum standards of adequacy.

5.2.2 Scope of the personal information protection law

As what been have clarified about the legislation of China's draft of personal information protection law above in the section of 5.1.1, there still remains several aspects to be covered in the process of formal legislation. Can China's personal protection law be applied outside China? Who can be the right holders under the personal protection law?

5.2.3 Handling of sensitive personal data

Sensitive personal data protection stands out as an important issue in information protection for the purpose that special kind of information should receive a higher level of protection, preventing personal rights from being infringed. Many international instruments and national legislations regulate special provisions on the protection of sensitive personal data. The DPD formulates the most comprehensive and stringent legal protection on this issue. The DPD qualifies "special categories of data" which actually are sensitive personal data.[53] In principle, the DPD prohibits the processing of such data, but exemptions are specified. The DPD also permits member states to specify additional exemptions which must be in the substantial public interest and must include suitable safeguards. Unless member states provide specific exemptions, such processing has to stop.

However, there is still a number of countries or regions who haven't put sensitive information under legislation. For example, such regulations are absent from APEC privacy protection principles, APEC Guidelines, and the laws in Japan, Korea and China Taiwan.[54] It is now time to take a look at the counterpart in Chinese draft. As is mentioned above in the section of 5.1.1, the protection of special categories of information has not

[53] Ariticle 8 of EU Directive 95/46/EC: Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade uion membership, and the processing of data concerning health or sex life.

[54] Supra footnote 38, p238

been regulated in the draft. Although the drafters and experts realize the notion and the necessity of protection of sensitive personal data, this issue remains to be specified and determined by the information and resource department of the State Council in the future.
The lack of the provisions of sensitive information protection has raised much controversy after the publication of the draft. It is the argument of some experts that these provisions must be included in the Chinese personal information protection law in order to obtain the full sense of protecting the fundamental individual rights stipulated by the Constitution and the real significance of the law. Otherwise, it will do harm the balance and harmonization between the private and public interests. At the same time, others argue that if the drafters adopt the definition of sensitive personal information, the personal information protection law will conflict with Constitution and basic political system including political opinions, religious or philosophical beliefs and etc. It seems impossible to adopt the specification of such protection of information unless the Constitution has been revised and the political system has been reformed.[55]

Consequently, if China wishes its information protection regime to be up to the level of "adequacy" for the purpose of the DPD, it is advised to regulate those special categories of information. So what definition of "sensitive data" should China adopt? How can the necessary protection be justified? Who has the authority to determine the application and exemptions? A few issues need to be solved.

5.2.4 International transfers of personal data

Due to the facility provided by the internet and computer technology for the transfer of personal data to all corners of the world, it becomes an indispensable issue to tackle the process of international trade and data protection regime. There are no restrictions at all on transfers to countries within the European Economic Area (the 25 members of the EU plus Norway, Iceland and Liechtenstein). Nowadays quite a few numbers of the cases are that companies based in EU are proscessing part of the personal data to third countries. If those

[55] Constitution of the PRC states that China shall ensure and uphold the leadership of the Communist Party of China, as well as communist political system. Thus all individuals' freedom must comply with this principle. The freedom of political opinions and relative expressions certainly cannot be accepted by legislation for the unification of whole jurisdiction.

third countries have no corresponding data protection law, the legal protection offered by the DPD would be void.

There is no definition of a transfer in either the 1984 Act or the EU Directive. It is not easy to devise the rules governing the international transfer of personal data that are both effective and not burdensome to operate. The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data adopts a broad statement of principles rather than detailed arrangements. The stipulations in the EU Directive are a serious attempt to come to terms with the issues of international transfers.

The DPD Article 25(1) stipulates the basic rule that the transfer of personal data to third countries may take place only if "the third countries in question ensures an adequate level of protection." In addition, the DPD Article 25(2) states that "adequacy" is to be assessed in the light of "all circumstances" surrounding the transfer. The Commission has the capacity to make findings of adequacy in relation to third countries. The standard it has applied for making such findings with respect to a country is that the country has generally applicable law equivalent to EU framework. And the DPD Ariticle 26 makes detailed provisions on the derogations of the authorization of the transfers of personal data to countries without an adequate level of protection where the data controller provides "adequate safeguards". Most of the provisions deal with the procedural arrangements for decision-making within the EU.

The Article 29 Working Party produced some helpful guidance on the interpretations of Article 25 and 26 of the EU Directive in July 1998 which has subsequently been relevant in making adequacy assessments and is referred to in later Commission decisions.[56]

Regarding the application of the rules, it remains a question that whether the adequacy of protection in third countries needs to be assessed by data protection supervisory authority before each transfer. Many member states tend to take the form of prior authorization from the supervisory authority. Others leave the initial decision on adequacy to be made by the data controller who is making the transfer, but allows for the challenge by the supervisory authority if needed. A further possible route to enable the transfer to countries without

[56] "Transfer of personal data to third countries: Applying Article 25 and 26 of the EU data protection directive"

adequate protection is the development of Binding Corporate Rules under which a global company is entitled to establish its own scheme of biding internal contracts which commit the organization to adhere to an appropriate data protection standard. The commission has expressed concern that some member states have taken a relaxed view of the prohibition clause. Meanwhile, business has been frustrated at the bureaucracy imposed on transfers and proposed to find more business-friendly ways of dealing with the issues.[57]

What's more, EU makes particular finding of adequacy in the US model. Even after several revised versions of the Safe Harbor Agreement, the Article 29 working Party is still quite skeptical about the level of adequacy and its enforcement in the long term given that there is no effective independent enforcement except those self-regulatory programs.[58]

In respect of the successes and difficulties on the provisions governing international data transfer by the DPD and other legal instruments, it has posed both an opportunity and challenge to the prospective Chinese Personal Information Protection Law. It is extremely important for China to meet the adequacy level of the DPD since European countries are among the biggest Chinese trade partners. If China continues to fail the standard of adequacy, the restriction of information flow will be likely a trade barrier of EU market in the long run. What provisions should China adopt in its law for regulating international transfers of personal data? Should China follows the EU approach on this matter? Should China require international transfers to be authorized in advance? Thus all these matters need further considerations providing that the present existed provisions in the Draft is far from being comprehensive and effective. They are stated as follows:

The Draft Article 48 authorizes the information resource department to restrict other processors from cross-border information transfer for meeting any of the following conditions:

a) national security and other significant national interests;
b) special requirements of the obligations of Chinese government originated from international law;
c) the states or regions that received personal information fail to provide adequate legal protection;
d) other circumstances regulated by the law.

---

[57] Rose Mary, Data Protection Law and Practice Third Edition, p298

[58] Supra footnote 40 p14

Information resource department of the State Council shall take charge of assessing and recognizing the malfunctions of country and region stipulated in c), as well as determining the detailed criteria, methods and procedures.

It is easily observed from the present draft that it lacks indispensable derogations from the provisions. In addition, too much discretionary power has been assigned to the information resource department without independence, limitation and elaboration of the power. All the above-mentioned problems will be readdressed with tentative solutions in the following section.

5.2.5 Executive Mechanisms

As discussed in 5.1.2, the DPD Article 28 provides that the member states should establish one or even more independent agencies to monitor the enforcement of personal information law. The establishment of a sound executive mechanism plays a decisive role in the whole picture of personal information protection.

Simply put, the enforcement of the law depends on two factors, one is finding out that whether the law is being complied with; the other is taking measures to guarantee the enforcement if it is not obeyed. Taking the second factor into consideration, the enforcement of data protection can be attained in two ways: either through the ordinary court system (administrative, civil or criminal) or through a specialized data protection supervisory authority.

Usually it is fairly common and convenient for those EU member states to establish special supervisory bodies as is the DPD stipulates. The independent supervisory authorities, under the self-determination and enforcement of respective member states, earn the power of investigation and intervention. Where there is a violation of the data protection law, it has the power to engage in legal proceedings or to bring the violation to the attention of the judicial authorities. The supervisory authorities are also required to deal with complaints about alleged breaches of data protection law. All the models of the exact enforcement bodies leave to the decisions of corresponding states themselves.

Given the present status of a Chinese enforcing agency, we have no special government agency that controls information resources. Moreover, the only specified government information resources department is not clearly provided detailed legal responsibilities in the draft. According to the Chinese situation, the agency can either be a newly established special agency or an inner department of common agencies such as the General Office or the Secretariat. So which authority can take the responsibility of enforcing the information protection law? What level of the executive authority will it carry? How to ensure the enforcement of Chinese personal information protection law? What kinds of expedients will be? These questions will be approached one by one as follows.

6 Legal propositions to China's Personal Information Protection Law

6.1 On international recognition of China’s personal information protection law

In order to determine the adequacy of data protection, China’s personal information protection law needs to comprise the following terms and conditions, which are mainly two sets of contents:

- the specific rules applicable
- the measures for ensuring the legal application

Referring to the DPD, China’s personal informational protection law should contain the following provisions:

- data protection principles set out in the DPD Article 6;

- provisions relating to transparency in the DPD Articles 10 and 11;

- provisions relating to security, as in DPD Article 17;

- data subjects’ rights of access, rectification and opposition, as in DPD Article 12;

- restrictions on international transfers of personal data as in DPD Article 25;

- derogations of the application of the law as in DPD Article 26.

Here are emphasized two special provisions for processing particular kinds of data in a third country.

- First, where sensitive personal data are involved, additional safeguards should be available. It is necessary to include this article because it is inevitable to process the sensitive information.
- Regarding direct marketing, it is fairly essential to stipulate that a person has the right to protect his information from being used for this purpose since selling or illegally disclosing personal information often occurs in current Chinese economic development.

6.2 On the scope of China's Personal Information Protection Law

Till now, there's no regulation in the draft to specify which law will be applied if Chinese personal data is processed outside China. For example, organizations that are based in China may have personal information processed outside China. Is Chinese law applicable to such processing? If the Chinese law is limited to the processing taking place in China, it might lead to many organizations deliberately arrange for their processing to take place outside China so as to avoid Chinese personal information law. Found in the DPD, Article 4 provides the rule that the law of the country in which the data controller is established governs data protection, irrespective of where the processing actually takes place. However, the absence of Chinese corresponding rules in the draft may lead to the avoidance of the Chinese law. Thus specific provisions need to be covered on preventing evasion of local information protection law through processing abroad.

Another quite controversial issue is whether the law should apply only to information of living individuals. What it should be the law concerning the information about the dead people? The DPD has no provisions for this, leaving it to the member states. UK excludes the dead person from the group of data subject.[59] Chinese draft also keeps silent on this matter. However, there have numerous notorious cases in China where privacy and right of reputation of the dead celebrities are violated.[60] And the close relatives of these dead persons have sued for the infringement of the dead's reputation right and also impose negative influence on them in terms of mental state and social life. It is worthy to be emphasized in Chinese privacy legislation due to Chinese traditions and philosophy. It is uphold from the ancient time that yearning and grief towards passing relatives is an important part of the spiritual interests of a living person. The strong sense of close family kinship makes the living person feel that the protection of the dead relative bears relations to the interests of the whole family. It should be taken into consideration that all natural

[59] Data subject means "an individual who is the subject of personal data". A data subject must be a living individual. (Data Protection Act 1998)
http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_act_legal_guidance.pdf (accessed 23th Nov.2009)

[60] On the protection of right of reputation of the dead people,
http://www.lawtime.cn/info/lunwen/mfrenquan/2006102653334.html (accessed 23th Nov.2009)

persons' right be protected. The provisions also should be applied to the dead for a certain period after death.

6.3 On the legislation of sensitive personal information

On the issue of the protection of sensitive data, the drafters actually provided their reasons for why not utilizing the notion of sensitive data in the Chinese legislation. One reason is the same as one school of thought which states that the sensitivity of any personal data can vary according to the circumstances where the data are processed. Secondly, in foreign legislation, sensitive personal information covers a wide range of contents, including political inclination, religion, freedom of joining associations, health, sexual life, justice and others. Nevertheless, if we adopt the same wide range of definitions of sensitive data, some conflicts might arise due to Chinese characteristic constitution and political system. Furthermore, the experts also suggested that special laws can be formed to settle the issues like the collection of personal medical information instead of a general provision on sensitive information in the personal information protection law.

Analyzing the complication of the legislation on both the world scale and for the Chinese national situation, I tend to suggest a combination model of comprehensive legislation, special legislation for specific categories of information, self-regulation and technological protection as well. What is the most important is that this model should be simple and flexible. In order to allow the flexibility and feasibility, the definition and the handling of sensitive data should be expressed on a level of principle, rather than in detailed stipulations. However, the control and the application of the principle are not easy. Given the wide diversity of the cases of sensitive information, the information protection authority should be empowered to specify safeguards to be applied in particular circumstances.

6.4 On the issue of transborder personal information protection

First of all, the Chinese Personal Information Protection Law should regulate the international transfers in a more comprehensive way rather than in simple and vague terms as expressed in the present draft. China needs to consider how to achieve an effective regulatory regime while keeping to minimum administrative burdens on both regulators

and organizations who wish to transfer personal data to third countries. It is advisable that the “adequacy” test should be adopted for controlling transfers of personal data to third countries in the Chinese legislation.

Thus, if an approach based on “adequacy” is adopted it is necessary to include other features which are essential parts of the EU specific derogations from the provisions. Namely, the consent of the data subject, the use of contracts and other instruments, such as binding corporate rules, containing data protection safeguards; the central approval of such instruments; the central designation of particular countries as providing adequate protection, whether for all transfers, or subject to conditions. All of these measures will help facilitate the legitimate international transfers of personal data.

With view to the issue of prior authorization, as mentioned above, some EU member states follow the practice of prior authorization to determine whether in a particular case a country provides adequate protection. This prior checking system seems to be fairly attractive from a managerial and administrative perspective. Nevertheless, it suffers from some serious negative aspects. Regarding the huge amount of international transfers happen every day, it is difficult and unrealistic to expect an effective system to be capable of handling such a large number of applications, even though various forms of exemptions are allowed. What’s more, any system of prior authorization will make constraint on time, thus having a harmful result on the related transactions.

On the part of Chinese legislation, prior authorization should be avoided, as the efficiency and applicability would suffer. A more flexible practice will be suggested to allow the initial decision on the adequacy to be made by the organization, meanwhile authorize the regulator to challenge those initial decisions if needed.

6.5 On the executive mechanism

It is practical to construct a comprehensive government information resources department on the basis of government reform and restructuring. The department needs to take the comprehensive responsibilities of the management of the information and the use of the technologies involved. Under that circumstance, some measures can be adopted to enhance the efficiency of the enforcement. A case in point is that Germany as well as each province

has authority with distinct responsibilities. A further feature of the German law is that the organizations in some cases are permitted to appoint some officials to carry out certain function of protecting data.[61] Independent of the organizations they work with, the officials are required to assist to solve the problem, record the organizational work and make public hearings of the questions. It has been regarded as a quite successful example of the cooperating work with the relevant supervisory authority, which has been followed by some other states like France, Luxembourg, the Netherlands and Sweden.

Likewise, inspired by the above German practice, it is sensible for the corresponding Chinese government agency to invite some interior information protection officers or experts to ensure the agency's compliance with the information protection regulations. The Chinese government information resources may establish a special information committee of interior officers or other related experts to handle the reconsideration of some case thus acting some of the management as well as enforcement. In such a case, the compliance with the law, also the transparency of the agency work will be hugely promoted.

Besides complaining to the supervisory authority, individuals may seek a remedy, including compensation, by going directly to court. However, recourse to supervisory authorities is free of charge compared with the high fee of court charges. An independent supervisory and executive agency is indispensable for China to ensure reliable enforcement of the law.

It might be predicted that there will be some difficulty in building an independent and sound executive authority immediately dedicated to both private and public sectors. If that is the case, some alternatives might be established to ensure the enforcement of the law. One approach might be to deal separately with the public and private sectors. The first draft of the Directive had separate provisions for the public sector and the private sector (although this approach was dropped in the course of negotiations). Some countries outside the EU, for example Canada, still have separate laws for the public and private sectors. It would be possible for China to consider this approach by limiting the remit of the supervisory authority to the private sector, at least initially. This should not prevent an "adequacy" decision being made for that part of the law, since there are already precedents

[61] Zhang Xinbao, EU-China Information Society Project, http://www.eu-china infso.org/UserFiles/File/Access%20to%20Government%20Information%20report.pdf (accessed 20th Oct. 2009)

for such decisions applying to some countries (for example, the US "safe harbor" arrangements, and the Canadian Personal Information Protection and Electronic Documents Act).[62]

Another possibility is to use alternative dispute resolution procedures (ADRs) to facilitate and accelerate the conflict resolution in information protection circumstances. Among various forms of ADRs, the most two common are arbitration and mediation. In arbitration, both sides are agreed by the contract they entered to let a third party decide how the dispute should be resolved. It will have a legal-binding effect on the resolution of the dispute. While in mediation, a third party is appointed to facilitate an agreement which is accepted by both parties with legal-binding effect.

Though ADRs are by no means substitutes to the normal measures, ADR is an effective and efficient way to solve the disputes. Before a sound and independent executive body is established in China, ADRs could play a very important role in assisting individuals in resolving their complaints.

[62] Supra footnote 61, p39

7 CONCLUSION

Privacy concerns stepped onto the world stage in the 1960s. Issues like what personal information can be collected, where and how it can be stored, who can have access to it, and what can be done to deal with it are continuously in the limelight of the world's discussion. Personal information, no matter recorded by automatic computer technology or by manual systems, constitutes consumers' access to credit and insurance, guides the search for the suspects, shapes the medical and health statistics, directs the attention of the businesses and so on. It is the significant interests and the uppermost individual human rights hidden behind that all these processes that require the sharp attention in law and policy in the world as a whole.

Consequently, corresponding legal protections are the reactions to the paramount issue. The DPD, the OECD Guidelines, the UN Guidelines and other international instruments as well as the respective nations' legislations have been established to govern the data protection. All these data protection laws share the common grounds that they will balance organization's need to use personal information with individuals' right to respect for their privacy.

Having been widely recognized and legally protected to a relatively large extent, the protection of personal information in China is still a fairly new issue in the academia as well as the public. With the expanding speed and range of the information flow under the economic globalization, the business value and credit value have been amplified to an unprecedented degree. Thus it has posed enormous challenges to the present society's information protection system. It has become controversy that how to balance the economic value and the individual rights of personal information under the principle that personal information is respected and protected as well as profited.

Due to the cultural traditions and political features, the protection of personal privacy and information has still not been widely recognized and respected by a large fraction of

population and not in the legislation. The private sector, organizations and public society still have taken active participation in the realization, legislation and implementation of issue.

Everyday a myriad of personal data is collected and processed through either a governmental agency, an organization authorized to carry out certain administrative functions, or some private companies. Being open to the world market and exploring it to a deeper extent, China brooks no delay in establishing a personal information protection system. Given the status quo of China, it is very urgent to enact the legislation of personal information law for the following reasons: The citizens have strengthened the consciousness of personal right with respect to the increasing cases of infringement of personal privacy and information abuse. Also, with the development of personal information sharing among government organs, how to balance between the protection of personal information and improvement of administrative efficiency is a big deal.

The great significance of the establishment of personal information protection law has been generally recognized in China. It will contribute to the sharing and free flow of information in the domestic market and world as large. It will substantially promote a healthy and sustainable development of China's E-Commerce and E-Governance. E-Commerce has been noted as a prime driving force for the economic growth in the 21st century. Likewise, E-Governance is indispensable to build up a high efficient and transparent government. It will also facilitate international exchange and keeps China in a favorable position in international relations and world market competition. On the arena of the world, the flow of information stands potentially as a trade barrier if a country lacks certain required level of information protection. Having heavier international pressure on personal information protection, China should take the initiative to reform and establish personal information protection law, rather than wait to be forced to change its current system.

To meet the strong voice both domestically and internationally, China finally formulates a draft of personal information protection law. Its effect as a milestone in the legislation of privacy protection in China cannot be overlooked. It marks a consensus on this issue in the society and the enhancement of the protection of Chinese human right. It proposed the concept

of information protection and formalized some new fields in the legislation, regardless of some inherent drawbacks. It is far from solving the current issues effectively, not to speak of meeting international data protection standards.
The Draft mainly covers the issue of determine the definition of the subject matter (personal information protection instead of privacy protection), the form of lawmaking (uniform lawmaking instead of separated lawmaking), the principles regarding the relation between personal information protection and information sharing and the management of cross-border data flow.

However, the draft suffers from a number of issues to be reconsidered and perfected. Chinese jurists and experts will dedicate themselves to the amendment and perfection on the current draft. And this paper provides some corresponding suggestions on the problems solving.

a. China should make an appropriate balance between personal information protection and maintenance of national security. Choice should be made in the personal protection law.

b. The protection of sensitive information should be integrated into the law. Issues like AIDS information of the patients are a typically controversy in the Chinese society. Nevertheless a flexible and principle-oriented legislation will be more suitable according to the complexity of the Chinese social and legal environment.

c. China should establish an independent executive agency with detailed and clear-cut legislation on what function it should fulfill. Moreover, other assistant strategies like establishing interior information protection personnel to control and promote the efficiency are suggested in the paper. The advice on the interim measure will also contribute to form an effective enforcement.

d. China should pay special attention to the international transfer of information in order to obtain the standard of adequacy, thus securing its favorable status in the world trade and other economic activities. Some supplementation should be made to the current draft. For example

the article of derogations and the avoidance of prior authorization requirement are advised in order to attain an effective and practical implementation.

e. Last but not the least, government and the public should stimulate the attention of the society at large to safeguard their personal rights to information and privacy. A larger number of organizations, educational bodies and private sector organizations should take more participation on the protection of the personal information and the legislation process by means of propaganda and publications.

BIBLIOGRAPHIES

1. Literature

Bygrave, Lee A,
Data Protection Law: Approaching Its Rational, Logic and Limits, Kluwer Law International, The Hague/London/New York 2002

Bygrave, Lee A,
Privacy Protection in a Global Context – A Comparative Overview, Scandinavian Studies in Law, 2004, vol 47, pp 319-348

James B.Rule and Graham Greenleaf,
Global Privacy Protection, The first Generation, Edward Elgar, Cheltenham, UK; Northampton, MA, USA, 2008

Li Changxi,
Internet Law-making of Personal Information Protection in China, Research on the Forefront of the Protection of Personal Information, Law Press China, 2006

Rosemary Jay,
Data Protection Law and Practice, Third Edition, London, Sweet & Maxwell, 2007

Warren, S.D and Brandeis, L.D,.
The Right to Privacy, Havard Law Review, 1980, vol 4

Yang Lixin
Discussion on Law of Personality Rights, Higher Education Press, 2005

Zhang Xinbao,
Legal Protection of the Right to Privacy, Qun Zhong Publishing House China, 2004

Zhang Xinbao
Status quo and Outlook on Personal Information Protection Legislation, available at: http://article.chinalawinfo.com/Article_Detail.asp?ArticleID=37590 (accessed 1, Oct, 2009)

Zhou Hanhua,
Personal Information Protection Act of China(Experts on) and the legislative Study Report, Law Press China, 2006

Zhou Hanhua,
Research on the Forefront of the Protection of Personal Information, Law Press China, 2006

2. Treaties/Statutes

APEC Privacy Framework and Guidelines, 2005

Administrative Reconsideration Law of PRC

Administrative Procedure Law of PRC

Constitution of the People's Republic of China

Criminal law of the People's Republic of China

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, adopted 24th October 1995

Data Protection Act 1998
http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_act_legal_guidance.pdf (accessed 23th Nov.2009)

General Principles of the Civil Law of PRC

Interpretation on Problem regarding the Ascertainment of Compensation Liability for Emotional Damage in Civil Torts of PRC

Opinions of the Supreme People's Cournt on Several Issues concerning the Implementation of the General Principles of the Civil Law People's Republic of China

Opinions of the Supreme People's Cournt on Several Issues for the Judgement of Case on Right to Reputation of PRC

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, adopted 23 September 1980

Postal law of the People's Republic of China

3. Websites

Cai Fang,
On the Concept of Privacy in China and the West, Journal of Jiangse Polytechnic University Social Science Edition,2007,vol.2, available at:http://scholar.ilib.cn/A-jssyhgxyxb-skb200702006.html (accessed 10th Oct,2009)

Case study: Discussion on personal privacy from the aspect of human flesh search engine. Available at http://www.chinaret.com/user/topic_view.aspx?id=b7a9dcd6-3827-4f83-8a4a-431d2b1514fa (accessed 15,Oct,2009)

China's Internet Users Increased To 298 Million In 2008, available at http://www.chinatechnews.com/2009/01/14/8507-chinas-internet-users-increased-to-298-million-in-2008(accessed 15th Oct,2009)

Feng Jianpeng,

Brief discussion on rivacy protection in the information era, available at:http://chinalawedu.com/news/2004_7%5C19%5C1639588312.htm (accessed 10th Oct,2009)

Graham Greenleaf,
Five years of the APEC Privacy Framework: Failure or promise?, (2009) Computer Law & Security Report 25 CLSR 28-43
http://www.sciencedirect.com/science?_ob=MImg&_imagekey=B6VB3-4VHYRH6 51&_cdi=5915&_user=674998&_orig=search&_coverDate=12%2F31%2F2009&_sk=99974 9998&view=c&wchp=dGLzVzz-zSkWA&md5=f8e761ab03ee1942a8f02c32790bc0ad&ie=/sdarticle.pdf (accessed 15th, Nov. 2009)

Lawmaker, advisor urge for better protection of personal information**,** available at http://news.xinhuanet.com/english/2009-03/04/content_10940007.htm (assessed 15th Oct,2009)

On the protection of right of reputation of the dead people, http://www.lawtime.cn/info/lunwen/mfrenquan/2006102653334.html (accessed 23th Nov.2009)

Paul De Hert and Vagelis Papakonstantinou,
"The data protection framework decision of 27 November 2008 regarding police and judicial cooperation in criminal matters – A modest achievement however not the improvement some have hoped for" 18 September 2009; available at http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6VB3-4X8524W-3&_user=10&_coverDate=09%2F30%2F2009&_rdoc=1&_fmt=full&_orig=search&_cdi=59 15&_sort=d&_docanchor=&view=c&_searchStrId=1056379020&_rerunOrigin=google&_acc t=C000050221&_version=1&_urlVersion=0&_userid=10&md5=e1e59775281146a5dc0bb34 4c11bf063 (accessed 10 Oct, 2009)

Roland Vogl,
The EU-US Privacy Controversy: a Question of Law or Governance?, May, 2000, p8
http://www.law.stanford.edu/publications/dissertations_theses/diss/VoglRoland-tft2000.pdf
(accessed 10th, Nov.2009)

State Information Development Strategy(2006-2020), May 19, 2006 available at:
http://www.cnii.com.cn/20050801/ca350966.htm (accessed 16 Oct, 2009)

Working Party, Article 29,
http://ec.europa.eu/justice_home/fsj/privacy/news/docs/pr_20_04_07_en.pdf (accessed 25th, Nov.2009)

Zhang Xinbao, EU-China Information Society Project, http://www.eu-china
infso.org/UserFiles/File/Access%20to%20Government%20Information%20report.pdf
(accessed 20th Oct. 2009)